INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 100-103

e-ISSN : 2583-1062

Impact Factor : 5.725

MODELING AND DETECTION OFFLOODING-BASED DENIAL-OF-SERVICE ATTACK IN WIRELESS AD HOC NETWORK USING BAYESIAN INFERENCE

A Dinesh Kumar[1], Dr.R.Shobarani[2], Dr.S.Geetha[3]

[1]Final Year M.Tech CFIS, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India.

[2]Professor, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India.

[3]Head of Department, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India.

ABSTRACT

Wireless ad hoc networks are widely useful in locations where the existing infrastructure is difficult to use, especially during the situations like flood, earthquakes, and other natural or man-made calamities. Lack of centralized management and absence of secure boundaries make these networks vulnerable to various types of attacks. Moreover, the mobile nodes used in these networks have limited computational capability, memory, and battery backup. Flooding-based denial-of-service (DoS) attack, which results in denial of sleep attack, targets the mobile node's constrained resources which results in excess consumption of battery backup. In SYN flooding-based DoS attack, the attacker sends a large number of spoofed SYN packets which not only overflow the target buffer but also creates network congestion. The present article is divided into three parts: mathematical modeling for SYN traffic in the network using Bayesian inference; proving the equivalence of Bayesian inference with exponential weighted moving average; and 3) develop an efficient algorithm for the detection of SYN flooding attack using Bayesian inference. Based on the comprehensive evaluation using mathematical modeling and simulation, the proposed method can successfully defend any type of flooding-based DoS attack in wireless ad hoc network with higher detection accuracy and extremely lower false detection rate.

1. INTRODUCTION

Cloud computing is a recent technology that aims at providing access to resources instantly as per the needs of the end users. Cloud enables its customers to make use of the resources that are widely distributed in the internet to perform computations without installing in their own PC's and has to pay only for the service they consumed. All the computational requirements will be taken care of by the cloud service providers and hence all the complexities involved will be hidden from the user. NIST identifies the five key characteristics of cloud computing as on- demand self- service, resource pooling, broad network access, rapid elasticity and measured service. Cloud offers services in three basic forms namely infrastructure (IaaS), platforms (PaaS) and Software (SaaS) and is on the stage of evolution to provide everything as a service (XaaS).

2. LITERATURE SURVEY

M.Khan et.al, in this paper we have made a review of various outlier detection techniques from data mining perspective. Existing studies in data mining focus generally on finding patterns from large datasets and using it for organizational decision making. However, finding exceptions and outliers did not receive much attention in the data mining field as other topics received. Finally, this paper concludes some advances in outlier detection recently.

Masud M.M et.al, botnet is a network of compromised hosts or bots, under the control of a human attacker known as the botmaster. Botnets are used to perform malicious actions, such as launching DDoS attacks, sending spam or phishing emails and so on. Thus, botnets have emerged as a threat to internet community. Peer to Peer (P2P) is a relatively new architecture of botnets. These botnets are distributed, and small. So, they are difficult to locate and destroy. Most of the recent works in P2P botnet are in the analysis phase. On the contrary, our work is aimed at detecting P2P botnets using network traffic mining.

3. EXISTING SYSTEM

In existing, DoS attack detection mechanism suggested for the Internet can be used for attack detection in wireless ad hoc network, but attacker trace back mechanism suggested for Internet is not effective for these networks due to limited resources and computational ability of node. An ATA and cumulative sum (CUSUM) algorithm for the detection of SYN flooding-based DoS attack. Since the threshold is set adaptively based on mean SAR, the ATA misinterprets attack traffic as normal traffic after some samples of attack traffic due to persistent attack which further

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 100-103

e-ISSN : 2583-1062

Impact Factor : 5.725

results in increased false alarm rate and lower accuracy. A mechanism for early detection of SYN flooding attack in mobile ad hoc network (MANET) by monitoring the number of SYN packets, SYN-ACK packets, and final ACK packets exchanged between a node and a multimedia server. The number of half-open connections was calculated by the multimedia server and a decision is made as malicious node if the number of half-open connection is greater than a threshold.

4. LIMITATIONS OF THE EXISTING SYSTEM

Existing method suffering from higher false alarm rate since legitimate nodes are mis detected as an attacker if the RREQ rate is greater than the computed threshold. Lack of centralized management and absence of secure boundaries make these networks vulnerable to various types of attacks.

5. PROPOSED SYSTEM

In proposed system, a novel method is proposed for modeling the SYN traffic in the network using Bayesian inference, and the mean of Bayesian inference is used as a metric for SYN arrival rate (SAR) in the incoming traffic which is discussed in Section III. Since exponential weighted moving average (EWMA) is a widely used method for the detection of flooding attack, the proposed article proved the equivalence of mean of Bayesian inference with EWMA using three lemmas. It is proved that EWMA is equivalent to the mean of Bayesian inference for normal traffic as well as for persistent attack traffic. A method to detect the presence of attack in the incoming traffic is addressed in the present article.

For normal traffic, mean of Beta distribution is computed for each sample to estimate the normal statistics of mean SAR. So for attack detection, mean of Beta distribution is slightly modified to detect the changes in the incoming traffic. As the number of SYN packets is more than the normal statistics for consecutive samples (indication of anomalous traffic), the computed mean till the last sample of normal traffic is stored. Subsequently, the mean for anomalous traffic was recomputed.

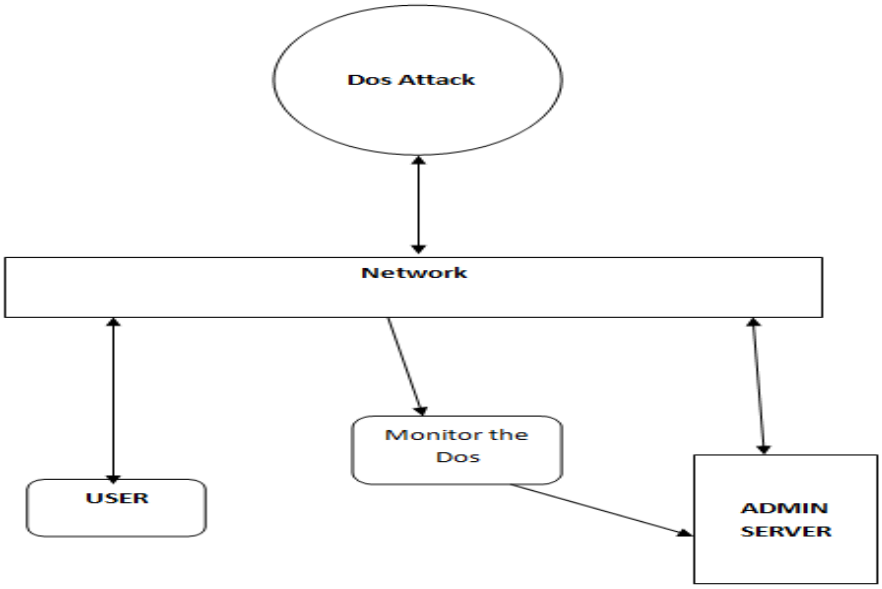

Figure 1. Architecture Diagram

5.1 List of Modules

- Login
- Register
- User Registration
- File Uploads
- View file details
- Threshold Dos attacks
- Graph details

5.2 Modules Description

Login

Logging in is usually used to enter a specific page, which trespassers cannot see. Once the user is logged in, the login token may be used to track what actions the user has taken while connected to the site.

User Registration

This module is User Registration; all the new users have to register. Each user is given a unique password with their user name. To access their account they have to give their valid username and password i.e. authentication and security is provided for their account.

File Uploads

In the file uploads module mainly designed to upload data from cloud. The method can also be used to find the misbehavior detection on data uploads from authorized to user to other user.

View File Details

In the uploaded file details to viewing file details for overall detailed showing user uploading file methods. User can easily to find out file details.

Threshold DOS Attacks

Threshold is a value. You associate the Threshold to a Statistic (Polled Data). When data is collected for that Statistic, it is compared with the associated Threshold value. If the collected data value does not suit the Threshold value then it indicates that this kind of data might lead to poor performance of the device or network. Here, the term "suit" is used as you can set up a Threshold value along with a level, such as the maximum value, the minimum value, and equal value.

Graph Details

In the details show in the graph in dos attackers shown in n number of attacking in networks on month and time details shown in the graph details. A chart, also called a graph, is a graphical representation of data, in which "the data is represented by symbols, such as bars in a bar chart, lines in a line chart, or slices in a pie chart .A chart can represent tabular numeric data, functions or some kinds of qualitative structure and provides different info.

6. CONCLUSION AND FUTURE ENHANCEMENT

In this paper we have applied the data mining techniques for identifying the Denial of Service attack. This type of attack is very dangerous as it jeopardizes the IT resources. It makes the server busy by imitation messages and repeated queries. The server is congested by traffic packets, in order to mitigate the server performance. In this research paper, we have discussed about Cyber security, cyber-crimes their types, clustering, outliers and pattern recognition. We have applied the famous data mining technique called as pattern recognition on the log file. We set a threshold value. If the number of similar requests are received at the server, which is greater than the threshold value, we assume this as an attack and the administrator is been informed. By this approach we can identify the denial of service attack easily as in DoS attack, the attacker or the hacker sends same multiple requests in order to mitigate the server performance.

7. REFERENCES

[1] Know Your Enemy: Learning about Security Threats, 2nd Edition.ISBN: 0321166469. The Honeypot Project 2004.

[2] M.Khan , S.K.Pradhan, M.A.Khaleel, “Outlier Detection for Business Intelligence using data mining techniques”, International journal of Computer Applications (0975 -8887), Volume 106- No. 2, November 2014.

[3] Masud, M.M, Gao, J.Khan, “Peer to Peer Botnet Detection for Cyber Security: A Data Mining Approach”. In proceedings: Cyber-security and information Intelligence research workshop. Oakridge national Laboratory, Oakridge May 2008.

[4] Internet Security Threat Report, Volume 21, April 2016, Symantec Crime Report.

[5] Ibrahim Salim, T.A.Razzack,”A study on IDS for Preventing denial of service attack using outliers techniques”, 2nd IEEE international conference on Engineering and technology, March 2016.

[6] S.S Rao, SANS Institute Infosec Reading Room.,”Denial of service Attack and mitigation techniques: Real time implementation with detailed analysis”, 2011.

[7] Data Mining:Concepts and Techniques, Third Edition, Jiawei Han and Micheline Kamber, ISBN-13, 9780123814791. [8] Mining of Massive Data Sets, Anand Rajaraman, Jure Leskovec, Jeffrey D. Ullman, 2014.

[8] Klein, A F. Ishikawa, and S. Honiden. Efficient heuristic approach with improved time complexity for qos-aware service composition. In ICWS, pages 436–443. IEEE, 2011.

[9] Tripathy, M.Khan, M.R.Patra, H.Fatima, P.Swain, “Dynamic web service composition with QoS clustering” IEEE, International Conference on Web services, 2014.

[10] O. Aciicmez, W. Schindler, and C. Koc, "Cache based remote timing attack on the AES," in Proc. 7th Cryptographers' Track RSA Conf. Topics Cryptology, 2007, pp. 271–286.

[11] AMD, "Advanced synchronization facility, proposed architectural specification (revision 2.1)," 2009. http://developer.amd. com/wordpress/media/2013/09/45432-ASF_Spec_2.1.pdf.

[12] C. Arnaud and P.-A. Fouque, "Timing attack against protected RSA-CRT implementation used in PolarSSL," in Proc. Cryptographers Track RSA Conf., 2013, pp. 18–33.

[13] J. Bauer, M. Gruhn, and [4] . Bauer, M. Gruhn, and F. Freiling, "Lest we forget: Cold-boot attacks on scrambled DDR3 memory," Digital Investigation, vol. 16, pp. S65–S74, 2016.

[14] Baumann A, M. Peinado, and G. Hunt, "Shielding applications from an untrusted cloud with Haven," in Proc. USENIX Symp. Operating Syst. Des. Implementation, 2014, pp. 267–283.

[15] M. Becher, M. Dornseif, and C. Klein, "Firewire: All your memory are belong to us," in Proc. CanSecWest Conf., 2005. http:// www.cansecwest.com/core05/2005-firewire-cansecwest.pdf.

[16] D. Bernstein, "Cache-timing attacks on AES," 2004. https://cr. yp.to/antiforgery/cachetiming-20050414.pdf.

[17] Birgisson A and U. Erlingsson, "An implementation and semantics for transactional memory introspection in Haskell," in Proc. ACM SIGPLAN 4th Workshop Program. Languages Anal. Security, 2009, pp. 87–99.

[18] Birgisson, M. Dhawan, U. Erlingsson, V. Ganapathy, and L. Iftode, "Enforcing authorization policies using transactional memory introspection," in Proc. 15th ACM Conf. Comput. Commun. Security, 2008, pp. 223–234.

[19] E.-O. Blass and W. Robertson, "TRESOR-HUNT: Attacking CPUbound encryption," in Proc. 28th Annu. Comput. Security Appl. Conf., 2012, pp. 71–78.